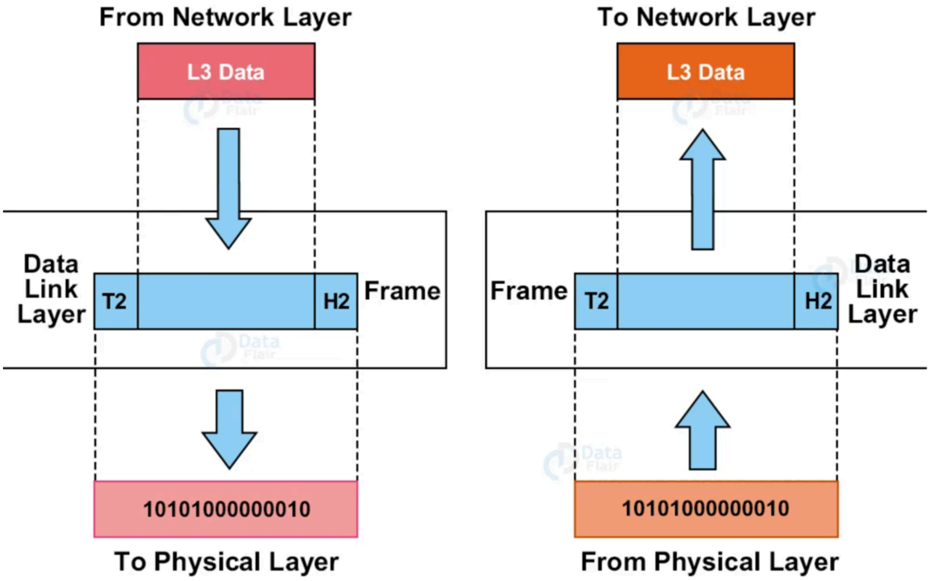
NETWORK LAYER



The Network Layer is the OSI model's third layer.

It responds to service requests from the transport layer and sends them to the data link layer.

The network layer is responsible for converting logical addresses into physical addresses.

It decides the path from the source to the destination and manages issues such as switching, routing, and data packet congestion.

The network layer’s primary function is to transport packets from the sending host to the receiving host.

Functions of Network Layer:

1. **Routing:** When a packet arrives at the router's input link, it is routed to the router's output link. A packet from S1 to R1, for example, must be sent to the next router on the way to S2.

2. **Logical Addressing:** The physical addressing is implemented by the data link layer, while the logical addressing is implemented by the network layer. Logical addressing is also utilized to distinguish between a system's source and destination.

   The network layer appends a header to the packet that contains the logical addresses of the sender and recipient.

3. **Internetworking:** The network layer’s primary function is to establish logical connections between different types of networks.

4. **Fragmentation:** It is the act of breaking down packets into the smallest individual data units that transit across various networks.

Forwarding and Routing:

A router is used on the network layer to forward packets.

A forwarding table is included on every router.

A router passes a packet by inspecting the header field and then indexing it into the forwarding table using the header field value.

The forwarding table value matching to the header field value specifies the router’s outgoing interface connection to which the packet is to be forwarded.

Network Layer Services:

1. **Guaranteed delivery:** This layer offers a service that ensures the packet arrives at its destination.

2. **Guaranteed delivery with bounded delay:** This service assures that the packet will arrive within the given host-to-host delay bound.

3. **In-Order packets:** This service assures that packets reach their destination in the order they were delivered.

4. **Guaranteed maximum jitter:** This service assures that the time between two consecutive transmissions at the sender equals the time between their receipt at the destination.

5. **Security services:** These are provided at the network layer through the use of a session key between the source and destination hosts.

The payloads of datagrams transmitted to the destination host are encrypted by the network layer of the source host.

The payload would subsequently be decrypted by the network layer at the target host.

In this manner, the network layer ensures data integrity and source authentication services.

Network Layer Addressing:

- One of the network layer’s primary duties is network addressing. Network addresses are always logical, or software-based.
- An interface is the barrier between the host and the connection. As a result, the host can only have one interface.
- A router differs from a host in that it has two or more connections to it.
- When a router forwards a datagram, the packet is sent to one of the links.
- An interface is the border between the router and the connection, and the router can have many interfaces, one for each of its links.
- Because each interface may transmit and receive IP packets, IP needs each interface to have an address.

Each IP address is 32 bits long and is expressed by “dot-decimal notation,” in which each byte is written in decimal form and separated by a period.

An IP address would be 192.10.216.9, where 192 is the decimal notation of the first 8 bits of an address and 10 is the decimal notation of the second 8 bits of an address.

IP Addressing:

IP addressing offers a technique for distinguishing between hosts and networks. Because IP addresses are issued in a hierarchical fashion, a host is always associated with a certain network. The host that needs to connect outside its subnet must know the target network address to which the packet/data is to be delivered.

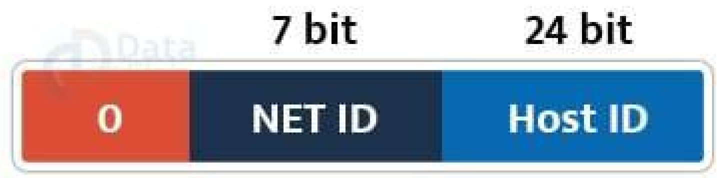
Hosts on separate subnets require a means for locating one another. DNS can handle this operation. DNS is a server that offers a distant host’s Layer-3 address that is mapped to its domain name.

Classful Addressing:

There are 2 parts of an IP Address:

- Network ID: Signifies number of networks
- Host ID: Signifies number of hosts

1. Class A:



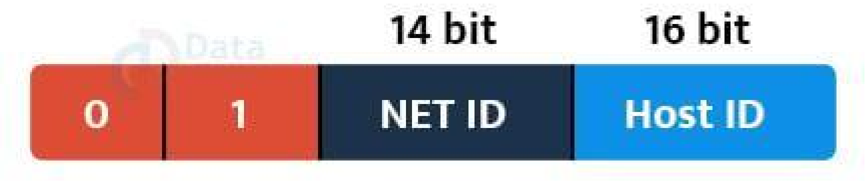
An IP address is allocated to networks with a high number of hosts in Class A. The network ID has an 8-bit length. The host ID has a length of 24 bits.

The first bit in the higher order bits of the first octet is always set to 0 in Class A, while the following 7 bits define the network ID. In any network, the host ID is determined by the remaining 24 bits.

Total number of networks = 2^7 = 128

Total number of hosts = $2^{24} – 2$ = 16777214

2. Class B:



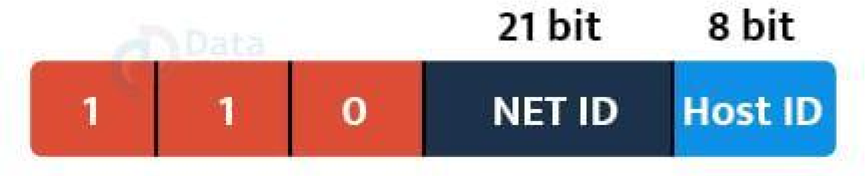
An IP address is issued to Class B networks, which range in size from modest to big. The Network ID is made up of 16 bits. The Host ID has a length of 16 bits.

The higher order bits of the first octet are always 10 in Class B, while the remaining 14 bits define the network ID. The last 16 bits define the Host ID.

Total number of networks = 2^{14} = 16384

Total number of hosts = $2^{16} – 2$ = 65534

3. Class C:



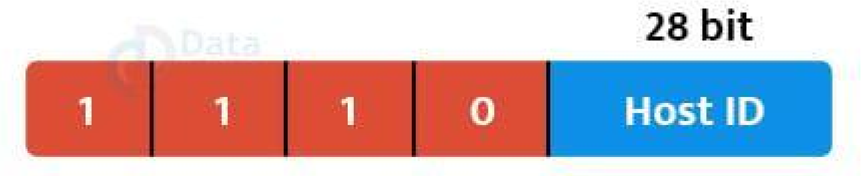
Only small-sized networks are allocated an IP address in Class C. The Network ID has a length of 24 bits. The host ID has an 8-bit length.

The higher order bits of the first octet are always set to 110 in Class C, while the remaining 21 bits define the network ID. The host ID, which consists of 8 bits, identifies the host in a network.

Total number of networks = 2^{21} = 2097152

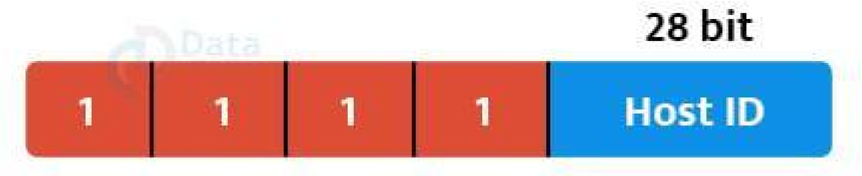
Total number of hosts = $2^{8} - 2$ = 254

4. Class D:



An IP address in Class D is designated for multicast addresses. It doesn’t have subnetting. The first octet’s higher order bits are always 1110, while the remaining bits decide the host ID in any network.

5. Class E:



An IP address is utilised in Class E for future usage or for research and development. It doesn’t have any subnetting. The first octet’s higher order bits are always 1111, while the remaining bits decide the host ID in any network.

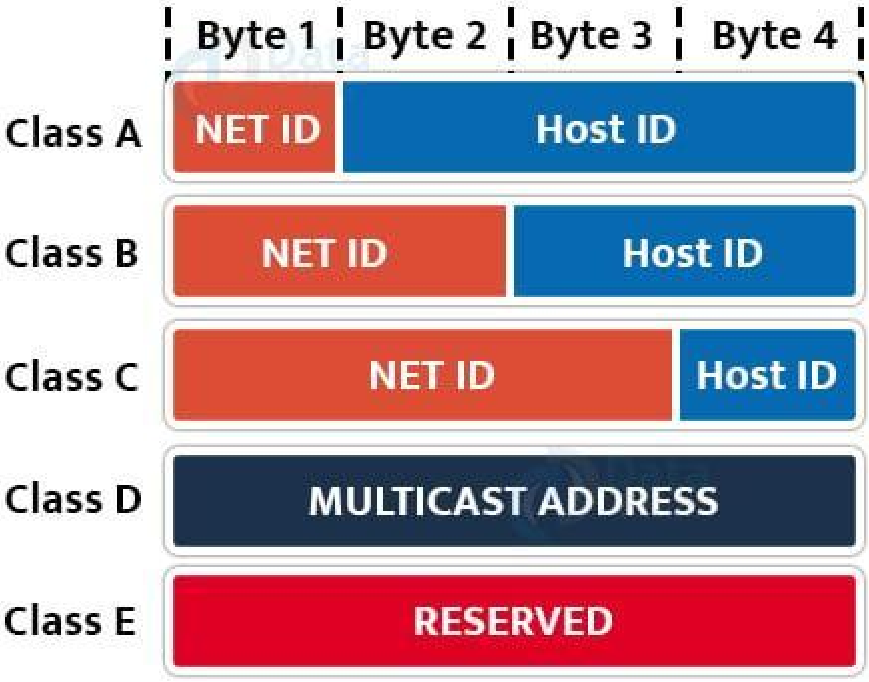
Network ID Rules:

Within any network, the Host ID must be unique. The Host ID with all bits set to 0 cannot be issued since it represents the network ID of the IP address. Because it is reserved for the multicast address, the Host ID with all bits set to 1 cannot be issued.

Host ID Rules:

Because 127 is utilised by Class A, the network ID cannot begin with that number. The Network ID with all bits set to 0 cannot be issued since it is needed to identify a specific host on the local network. Because it is reserved for the multicast address, the Network ID with all bits set to 1 cannot be issued.

Classful Addressing:



Classful addressing is a concept that splits the IPv4 address space into five classes: A, B, C, D, and E. This idea is now obsolete and has been superseded by classless addressing.

Prior to 1993, IP addresses used classful addressing, in which classes have a predetermined number of blocks and each block has a fixed number of hosts.

Classless Addressing

Classless Addressing is an improved IP Addressing system.

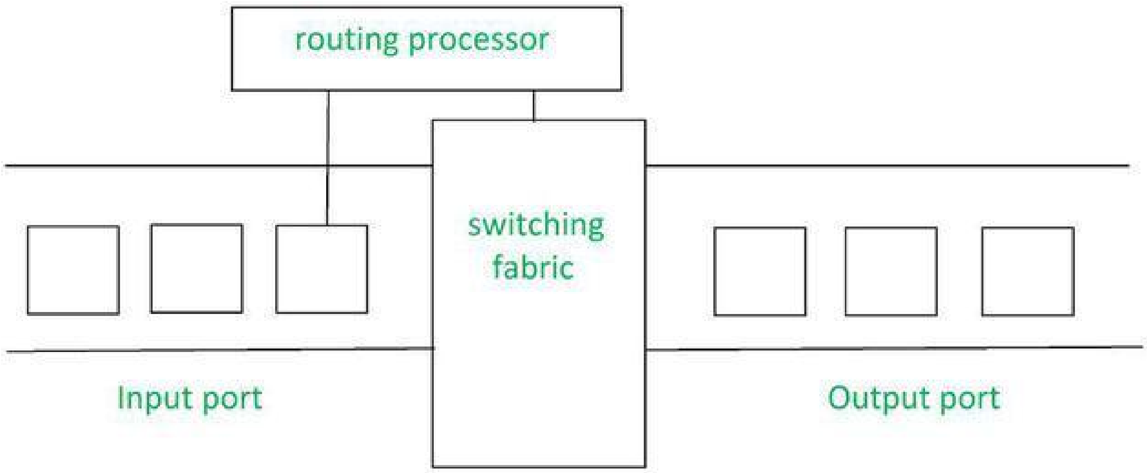
- It makes the allocation of IP Addresses more efficient.
- It replaces the older classful addressing system based on classes.
- It is also known as Classless Inter Domain Routing (CIDR).

CIDR Block

When a user asks for specific number of IP Addresses,

- CIDR dynamically assigns a block of IP Addresses based on certain rules.
- This block contains the required number of IP Addresses as demanded by the user.
- This block of IP Addresses is called as a CIDR block

Routers



Architecture of Router

A generic router consists of the following components:

Input Port: This is the interface by which packets are admitted into the router, it performs several key functions as terminating the physical link at the router.

Switching Fabric: This is the heart of the Router, it connects the input ports with the output ports. It is kind of a network inside a networking device. The switching fabric can be implemented in several ways some of the prominent ones are:

Switching via memory: In this, we have a processor which copies the packet from input ports and sends it to the appropriate output port. It works as a traditional CPU with input and output ports acting as input and output devices.

Switching via bus: In this implementation, we have a bus that connects all the input ports to all the output ports. On receiving a packet and determining which output port it must be delivered to, the input port puts a particular token on the packet and transfers it to the bus. All output ports can see the packets but they will be delivered to the output port whose token has been put in, the token is then scraped off by that output port and the packet is forwarded

Switching via interconnection network: This is a more sophisticated network, here instead of a single bus we use a 2N bus to connect n input ports to n output ports.

Output Port: This is the segment from which packets are transmitted out of the router. The output port looks at its queuing buffers (when more than one packets have to be transmitted through the same output port queuing buffers are formed) and takes packets, does link layer functions, and finally transmits the packets to an outgoing link.

Routing Processor: It executes the routing protocols, and it works like a traditional CPU. It employs various routing algorithms like the link-state algorithm, distance-vector algorithm, etc. to prepare the forwarding table, which is looked up to determine the route and the output port.

Routing is the ability to forward IP packets—a package of data with an Internet protocol (IP) address—from one network to another. The router's job is to connect the networks in your business and manage traffic within these networks. Routers typically have at least two network interface cards, or NICs, that allow the router to connect to other networks.

Speeding data across networks

Routers figure out the fastest data path between devices connected on a network, and then send data along these paths. To do this, routers use what's called a "metric value," or preference number. If a router has the choice of two routes to the same location, it will choose the path with the lowest metric. The metrics are stored in a routing table.

Creating a routing table

A routing table, which is stored on your router, is a list of all possible paths in your network. When routers receive IP packets that need to be forwarded somewhere else in the network, the router looks at the packet's destination IP address and then searches for the routing information in the routing table.

Types of Routing

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. The software based routers have limited functionality and limited scope.

A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination.

In case there are multiple path existing to reach the same destination, router can make decision based on the following information

1. Hop Count:

A hop count is a statistic that describes the number of trips through internetworking devices such as routers that a packet must make in order to go from source to destination.

If the routing protocol uses hop count as a major metric value, the path with the fewest hops will be deemed the optimal way to take from source to destination.

2. Delay:

It is the amount of time it takes a router to process, queue, and transmit a datagram to an interface.

This measure is used by protocols to calculate the delay values for all links along the path from beginning to finish.

The path with the shortest delay will be deemed the best path.

3. Bandwidth:

The bandwidth of the link is the capacity of the link.

Bits per second are used to measure bandwidth.

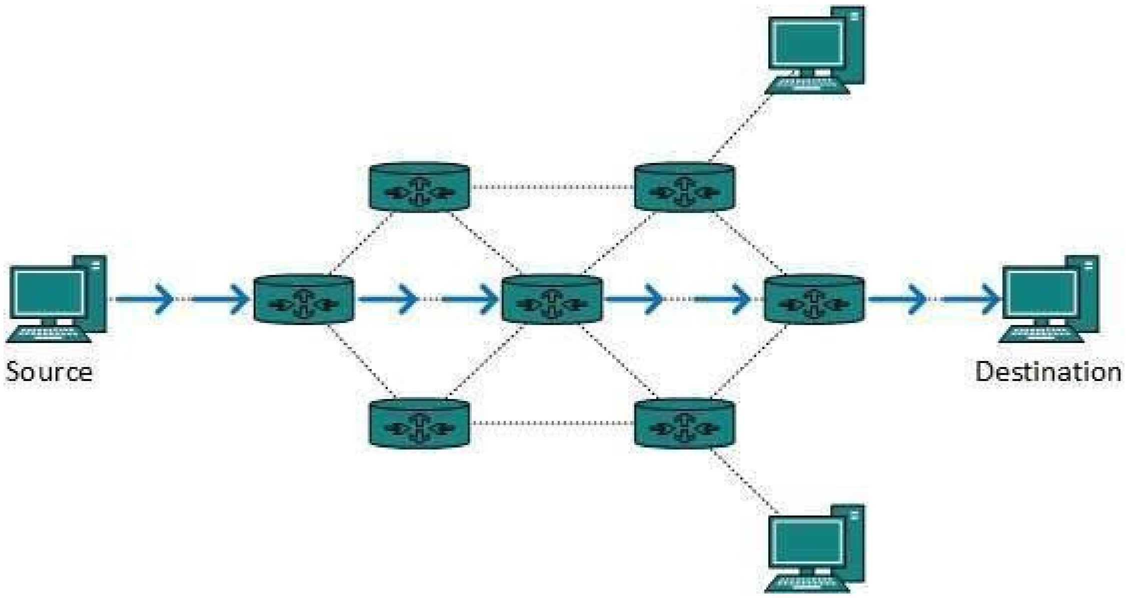
The protocol will assess the bandwidth capacity of each connection along the way, and the route with the highest total bandwidth will be regarded as the optimal route.

4. Load:

Load refers to how busy a network resource, such as a router or network link, is. It may be calculated in a number of ways, including CPU usage and packets processed per second.

Unicast routing

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.



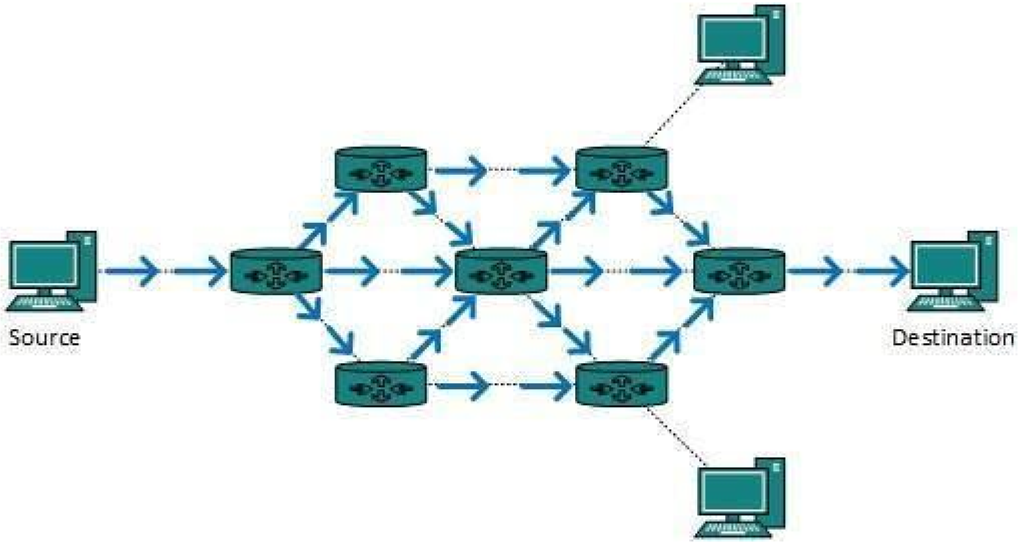
Broadcast routing

By default, the broadcast packets are not routed and forwarded by the routers on any network. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices.

Broadcast routing can be done in two ways (algorithm):

- A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting.

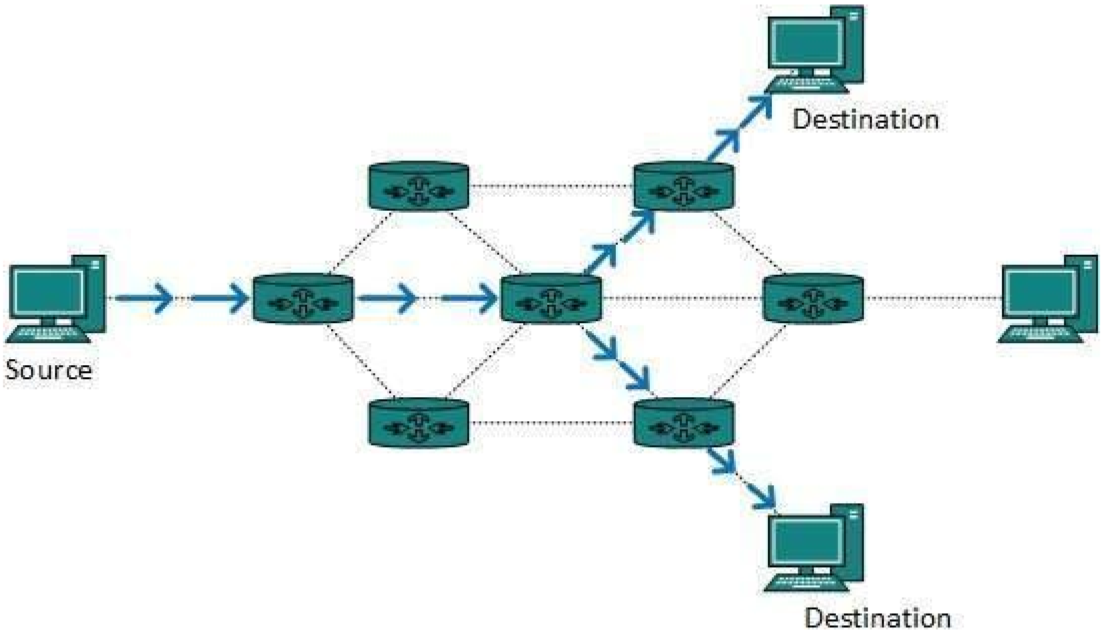
  This method consumes lots of bandwidth and router must destination address of each node.
- Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way.



This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers. Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

Multicast Routing

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.

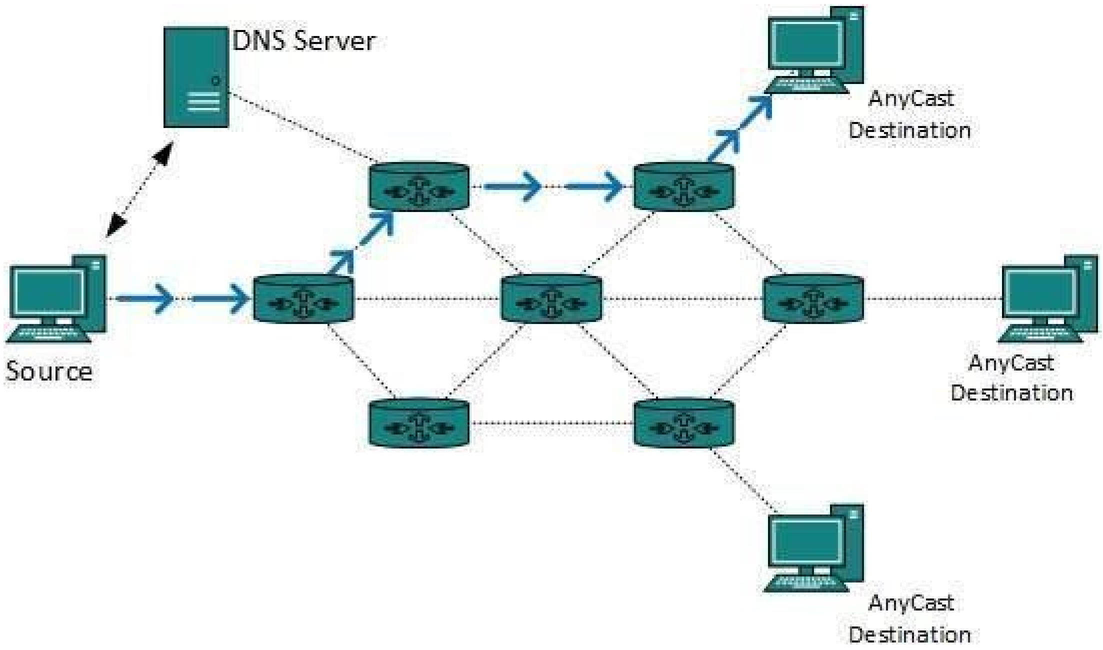


The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

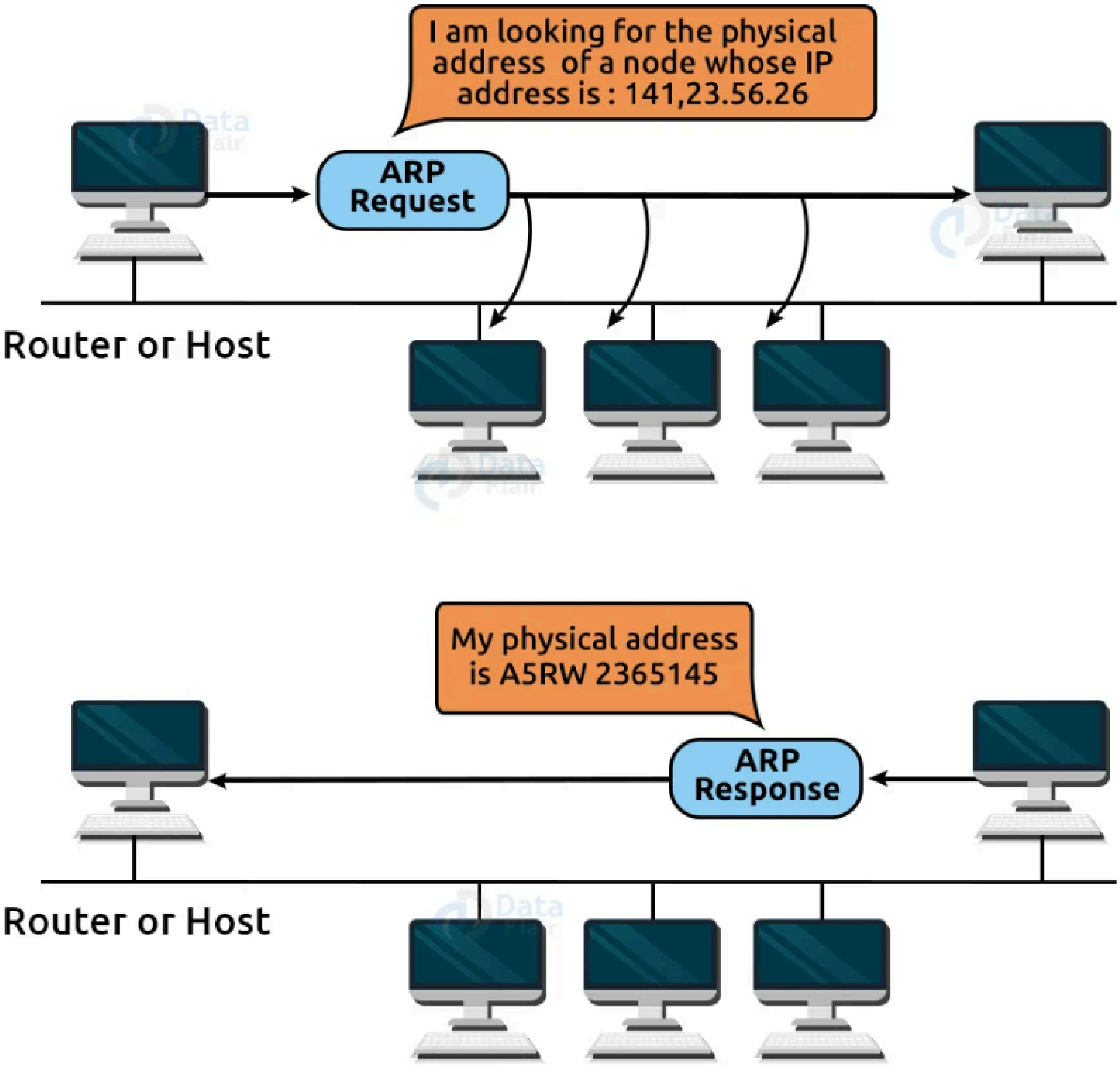
Anycast Routing

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology.



Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.

Address Resolution Protocol.


I am looking for the physical address of a node whose IP address is : 141,23.56.26
ARP Request
Router or Host
My physical address is A5RW 2365145
ARP Response
Router or Host

It is used to link an IP address to a MAC address. The MAC address etched on the NIC identifies each device on the network. As a result, we may argue that devices require the MAC address in order to communicate on a local area network. The MAC address may be readily modified.

For example, if a machine's NIC breaks, the MAC address changes but the IP address remains unchanged. When an internet address is known, ARP is used to determine the MAC address of the node.

Working of ARP:

The device will first check its internet list, known as the ARP cache, to see whether an IP address includes a matching MAC address. It will use the command arp-a to check the ARP cache on command prompt.

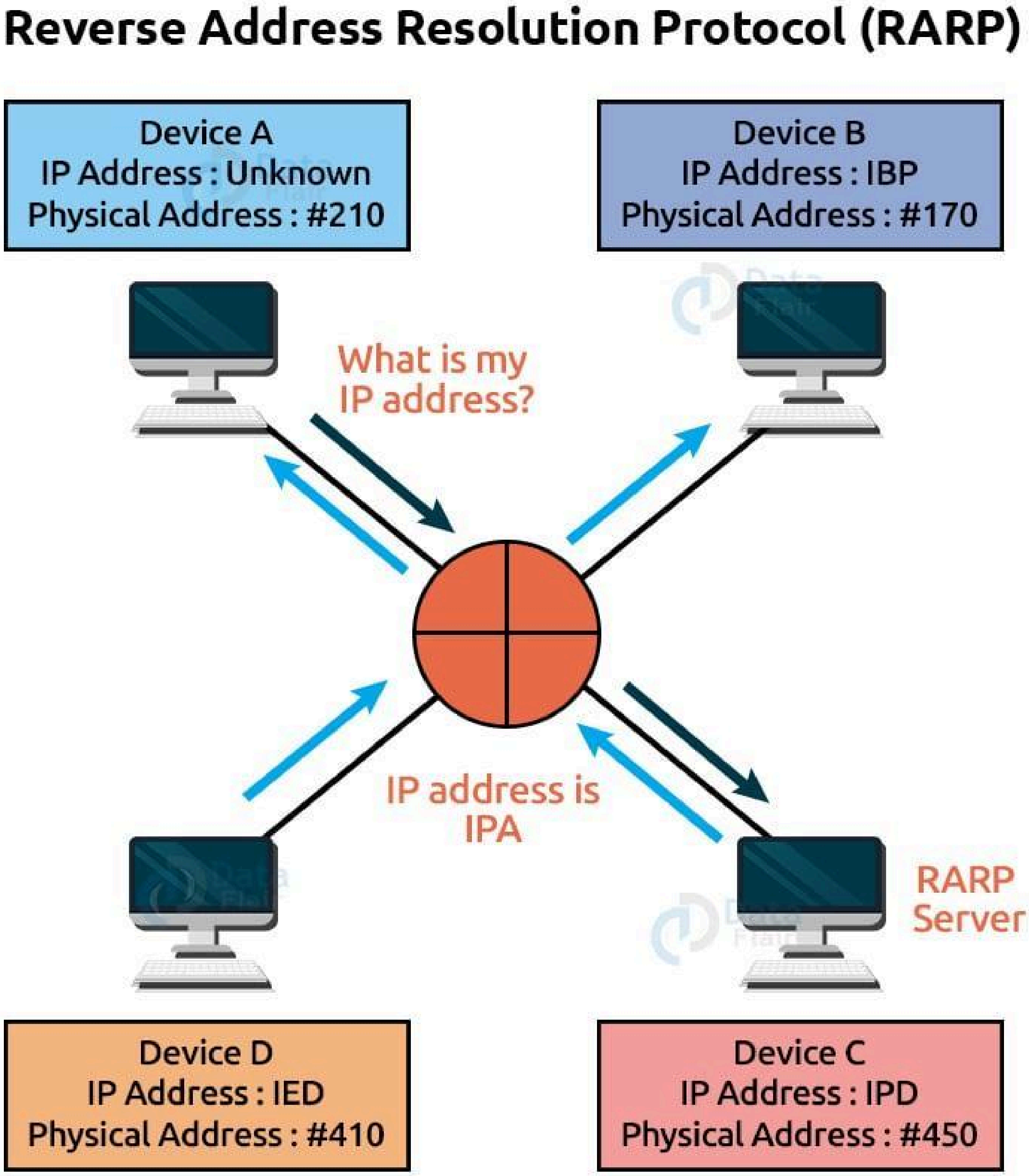
If the ARP cache is empty, the device broadcasts the message to the whole network, requesting a matching MAC address from each device. The device with the matching IP address will then respond with its MAC address to the sender. Once the MAC address is received by the device, communication between two devices is possible.

If the device receives the MAC address, it stores the MAC address in the ARP cache. Using the command arp -a, we may examine the ARP cache in the command prompt.

Types of ARP entries:

Dynamic entry: A dynamic entry is one that is produced automatically when a sender broadcasts their message to the whole network. Dynamic entries are not permanent and are deleted on a regular basis.
Static entry: This is an entry in which the IP to MAC address relationship is manually entered using the ARP command tool.

2. Reverse Address Resolution Protocol (RARP):



Reverse Address Resolution Protocol is the protocol used to acquire an IP address from a server. The RARP protocol uses a message format similar to the ARP protocol. RARP frames, like ARP frames, are transferred from one computer to another in the data section of a frame.

If the host wishes to know its IP address, it broadcasts to the whole network the RARP inquiry packet containing its physical address. The RARP packet is recognised by a RARP server on the network, which responds with the host IP address.

3. Internet Control Message Protocol (ICMP):

ICMP is an abbreviation for Internet Control Message Protocol. The Internet Control Message Protocol (ICMP) is a network layer protocol that hosts and routers utilize to transmit alerts of IP datagram issues back to the sender.

To determine if the target is accessible and responding, ICMP employs echo test/reply.

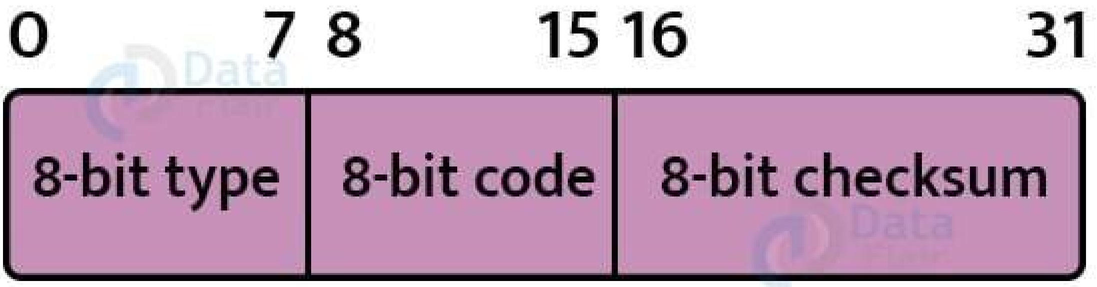
ICMP handles both control and error messages, although its primary role is to report errors rather than to fix them.

An IP datagram has both the source and destination addresses, but it does not know the address of the previous router through which it was transmitted. As a result, ICMP can only transmit messages to the source and not to the immediate routers.

The error messages are communicated to the sender using the ICMP protocol. Errors are returned to the user processes as a result of ICMP packets.

ICMP messages are sent as part of an IP datagram.

Structure of ICMP Message:



- The first field indicates the message's nature.
- The second column specifies the reason for sending a certain message type.
- Checksum field contains the checksum for the whole ICMP message.

Types of Errors Reported by ICMP:

a. Redirection: When a host has a tiny routing table, a redirection message is generated. When the host has a restricted number of entries and transmits the datagram to the incorrect router. When a router gets a datagram, it forwards it to the appropriate router and sends the "Redirection message" to the host in order to update its routing table.

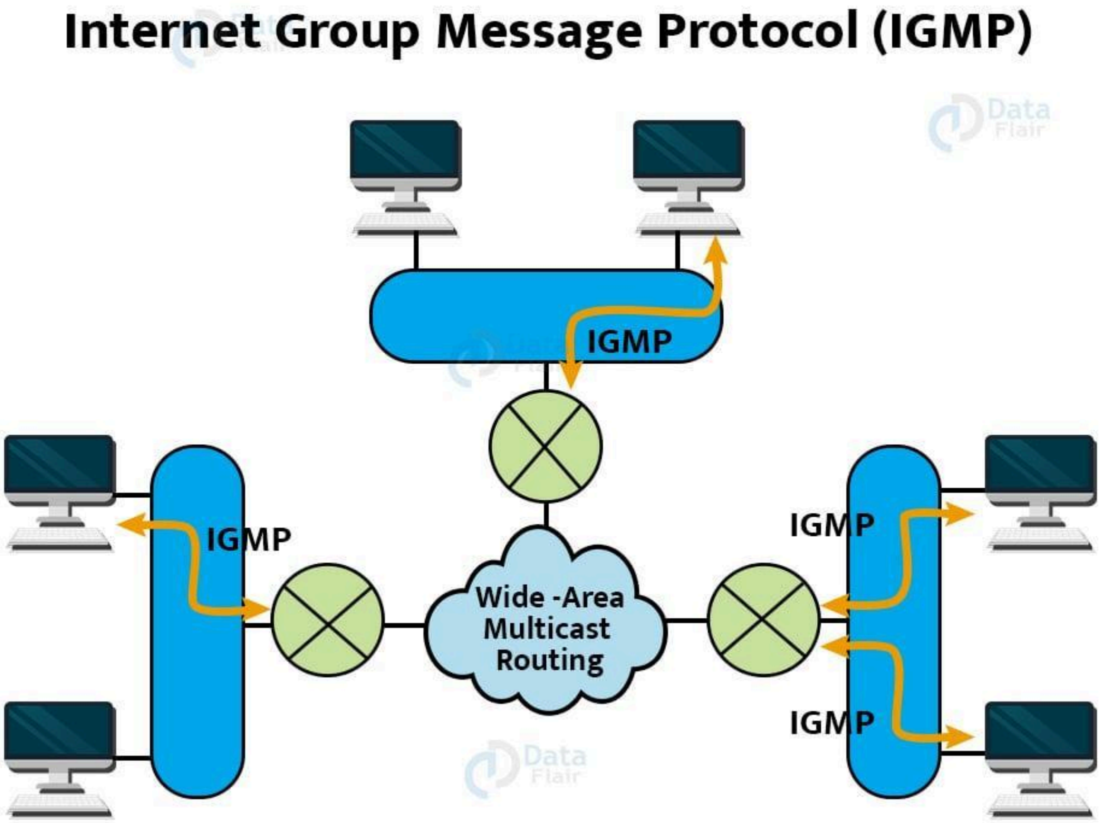
b. Parameter Problems: When a router or host detects a missing value in an IP datagram, the router discards the datagram and sends the "parameter issue" message back to the originating host.

c. Time Exceeded: Another name for Time Exceeded is "Time-To-Live." It is a parameter that specifies how long a packet should be kept before being discarded.

d. Destination Unreachable: When the destination cannot be reached, the message "Destination Unreachable" is delivered from the receiver to the sender, or the packet is discarded.

e. Source Quench: The source quench message's aim is to control congestion. The message is delivered from the overburdened router to the source host in order to lower the transmission rate. ICMP will take the IP address of the rejected packet and append the source quench message to the IP datagram to notify the source host that its transmission rate has been reduced. The source host will lower the transmission rate so that the router is not congested.

4. Internet Group Message Protocol (IGMP):

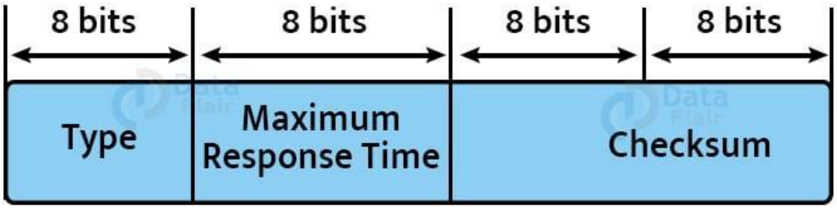

Internet Group Message Protocol (IGMP)
IGMP
IGMP
IGMP
IGMP
Wide -Area Multicast Routing

IGMP is an abbreviation for Internet Group Message Protocol. The IP protocol allows for two kinds of communication:

- Unicasting refers to communication between a single sender and a single recipient. As a result, we may call it one-to-one communication.
- Multicasting occurs when a sender wishes to deliver the same message to a large number of recipients at the same time. This is known as multicasting, and it involves one-to-many communication.

Hosts and routers utilise the IGMP protocol to support multicasting and identify hosts in a LAN that are members of a group.

Structure of IGMP Message:



Type: It specifies the kind of IGMP message. IGMP messages are classified into three types: Membership Query, Membership Report, and Leave Report.

Maximum Response Time: Only the Membership Query message uses this field. It specifies how long the host can wait before sending the Membership Report message in response to the Membership Query message.

Checksum: It determines the full payload of the IP datagram that contains the IGMP message.

Group Address: The behaviour of this field is determined on the kind of message transmitted.

Membership Query: The group address for Membership Query is set to zero for General Query and to multicast group address for a particular query.

Membership Report: The group address for Membership Report is set to the multicast group address.

Leave Group: It is set to the multicast group address for Leave Group.

IGMP Messages:

Membership Query Message

A router sends this message to all hosts on a local area network to identify the set of all multicast groups that the host has joined. It also checks if the hosts on a connected interface have joined a certain multicast group.

The group address in the query is zero because the router expects one answer from a host for each group on that host that has one or more members.

Membership Report Message

The host sends a membership report message in response to the membership query message.

When a host wants to join a multicast group without waiting for a membership question message from the router, it can emit membership report messages.

A router, as well as all hosts on a connected interface, get membership report messages.

Each membership report message contains the multicast address of a particular group in which the host wishes to participate.

The IGMP protocol is unconcerned with which hosts have joined the group or how many hosts are in a single group. It only concerns if one or more connected hosts are members of a single multicast group.

A router’s membership Query message includes a “Maximum Response time.” The host waits for a random length of time ranging from 0 to the maximum response time after receiving a membership inquiry message and before delivering the membership report message. If a host notices that another associated host has sent the “Maximum Report message,” it discards its own since the attached router already knows that one or more hosts have joined a single multicast group. This is referred to as feedback suppression. It optimises efficiency by eliminating the needless sending of a “Membership Report message.”